

U.S. Department of Commerce, Patent and Trademark Office (PTO Form 1449 modified)		Docket No. SRI 4374-2	Serial No. 09/996,154
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Applicant Porras, et al.	Confirmation No.: 2117
(Use several sheets if necessary)		Filing Date November 28, 2001	Group 2182
Examiner			



U.S. Patent Documents							
*Examiner Initial		Document Number	Issue Date	Applicant(s) Name	Class	Subclass	Filing Date If Appropriate
~	A1	5,440,723	08/08/1995	Arnold et al.	395	181	
↓	A2	2003/0145226	07/31/2003	Bruton, III et al.	713	201	01/28/2002
	A3	2003/0172166	09/11/2003	Judge et al.	709	229	03/08/2002
	A4						
	A5						NOV 20 2003

RECEIVED

Foreign Patent Documents							Technology Center 2100	
*Examiner Initial		Document Number	Date	Country	Class	Subclass	Translation	
							YES	NO
m	B1	03/077071	09/18/2003	WIPO	G06F	—	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	B2						<input type="checkbox"/>	<input type="checkbox"/>
	B3						<input type="checkbox"/>	<input type="checkbox"/>
	B4						<input type="checkbox"/>	<input type="checkbox"/>

Technology Center 2100

OTHER ART		
*Examiner Initial		Including Author, Title, Date, Pertinent Pages, Etc.
hw	C1	Almgren, et al., "A Lightweight Tool for Detecting Web Server Attacks," Network and Distributed Systems Security (NDSS 2000) Symposium Proceedings, 157-170, 2000
	C2	Almgren, et al., "Application-Integrated Data Collection for Security Monitoring," From <i>Recent Advances in Intrusion Detection (RAID 2001)</i> , Springer, Davis, California, October 2001, pg 22-36
	C3	Daniels, et al., "A Network Audit System for Host-Based Intrusion Detection (NASHID) in Linux," 16 th Annual Computer Security Application Conference (ACSAC'00) December 11-15, 2000, New Orleans, LA
	C4	Daniels, "Identification of Host Audit Data to Detect Attacks on Low-Level IP Vulnerabilities," J. Computer Security, 7(1): 3-35, 1999
	C5	Dayioglu, "APACHE Intrusion Detection Module," http://yunus.hacettepe.edu.tr/~burak/mod_id/ , Date Unknown, Downloaded November 10, 2003
	C6	Hollander, Y., "The Future of Web Server Security: Why your Web site is still vulnerable to attack," http://www.cgisecurity.com/lib/wpfuture.pdf , allegedly posted 2000
	C7	Lindqvist, et al., "eXpert-BSM: A Host-based Intrusion Detection Solution for Sun Solaris," Proc. 17 th Annual Computer Security Application Conference, pg 240-251, New Orleans, LA, December 10-14, 2001

U.S. Department of Commerce, Patent and Trademark Office		Docket No.	Serial No.
(PTO Form 1449 modified)		SRI 4374-2	09/996,154
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Applicant Porras, et al.	Confirmation No.: 2117
(Use several sheets if necessary)		Filing Date	Group
Examiner		November 28, 2001	2182

nr	C8	Munson, et al., "Watcher: The Missing Piece of the Security Puzzle," Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), December 10-14 2001, New Orleans, LA, pp 230-239, IEEE Press.
	C9	Porras et al, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," 20 th NISSC - October 9, 1997, pg. 353-365.
	C10	Tener, "AI and 4GL: Automated Detection and Investigation Tools", Proceedings of the IFIP Sec. '88, Australia, 1989, pp 23-29.

Examiner	Date Considered 10/31/03
----------	--------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

RECEIVED

NOV 20 2003

Technology Center 2100